

# Quantum Cryptography: from Theory to Practice

Hoi-Kwong Lo and Norbert Lütkenhaus

*Center for Quantum Information and Quantum Control,  
Department of Physics and Department of Electrical & Computer Engineering,  
University of Toronto, Toronto,  
Ontario, M5S 3G4, Canada*

*and*

*Institute for Quantum Computing & Department of Physics and Astronomy,  
University of Waterloo,  
200 University Ave. W. N2L 3G1*

(Dated: February 1, 2008)

Quantum cryptography can, in principle, provide unconditional security guaranteed by the law of physics only. Here, we survey the theory and practice of the subject and highlight some recent developments.

PACS numbers:

"The human desire to keep secrets is almost as old as writing itself." [1] With the advent in electronic commerce, the importance of secure communications via encryption is growing. Each time when we go on-line for internet banking, we should be concerned with communication security. Indeed, methods of secret communications were used in many ancient civilizations including Mesopotamia, Egypt, India and China. Legends say that Julius Caesar used a simple substitution cipher in his correspondences. Each letter is replaced by a letter that followed it three places alphabetically. For instance, the word LOW is replaced by ORZ because the first letter "L" in LOW is replaced by  $L \rightarrow M \rightarrow N \rightarrow O$ , etc. Regardless of the size of the shift, the illustrated method is still called Caesar's cipher.

Let us introduce the general problem of secure communication. Suppose a sender, Alice, would like to send a message to a receiver, Bob. An eavesdropper, Eve, would like to learn about the message. How can Alice prevent Eve from learning her message?

A standard method is encryption. Alice uses her encryption key (some secret information) to transform her message (a plaintext) into something (a ciphertext) that is unintelligible to Eve and sends the ciphertext through a communication channel. Bob, with his decryption key, recovers Alice's message from the ciphertext. For instance, in Caesar's cipher, the key takes a value between 1 and 26, which denotes the size of the shift.

Since encryption machines may be captured, in modern cryptography, it is standard to assume that the encryption method is known and the security of the message lies on the security of the key. For instance, we assume that Eve knows that Caesar's cipher is being used, but she does not *a priori* know the value of the key. Note that Caesar's cipher is not that secure because the number of all possible key values is so small (only 26) that Eve can easily try all possible values.

Throughout the history of cryptography, many ciphers have been invented and believed for a while to be unbreakable. Almost all have subsequently been broken,

with disastrous consequences to the unsuspecting users. For instance, in the Second World War, the Allies' breaking of the German Enigma code contributed greatly to the ultimate victory of the Allies. The first lesson in cryptography is: never under-estimate the ingenuity and efforts that your enemies are willing to spend on breaking your codes.

Unbreakable codes do exist in conventional cryptography. They are called one-time pads and were invented by Gilbert Vernam in 1918: A message is first converted into a binary form (i.e., a string consisting of 0's and 1's) by a publicly known method. The key is another sequence of 0's and 1's of the same length. For encryption, Alice combines each bit of the message with the respective bit of the key by using addition modulo 2 to generate the ciphertext. For decryption, Bob combines each bit of the ciphertext with the respective bit of the key by using addition modulo 2 to generate the plaintext.

For one-time pad to be secure, it is important that a key is never re-used. This is why it is called a one-time pad. Why re-using a key would make the scheme insecure? Suppose the same key,  $k$ , is used to encrypt two different messages,  $m_1$  and  $m_2$ . Then, the ciphertexts,  $c_1 = m_1 \oplus k$  and  $c_2 = m_2 \oplus k$ , are transmitted in public. An eavesdropper can simply take the addition modulo 2 of the two ciphertexts to obtain  $c_1 \oplus c_2 = m_1 \oplus k \oplus m_2 \oplus k = m_1 \oplus m_2$ . But, this allows Eve to learn some non-trivial information, namely the parity, about the two original messages.

## I. KEY DISTRIBUTION PROBLEM

The one-time pad has a serious drawback: it presupposes that Alice and Bob share a random string of secret, a key, before the actual transmission of the message. So, the introduction of the one-time pad shifts the problem of secure communication to the problem of secure key distribution. This is called the key distribution problem. In top secret applications, key distribution is

often done by trusted couriers. Recall that in one-time pad, a key must be as long as a message. Sending long keys by trusted couriers is clearly rather inconvenient.

All conventional (classical) key distribution schemes are fundamentally insecure because there is nothing to prevent an eavesdropper from making a copy of the key during the key distribution process. Indeed, trusted couriers could be bribed or compromised. So, the users can never be sure about the security of a key.

How may one solve the key distribution problem? Around 1970s, mathematicians invented public key cryptography. In public key cryptography, there are two different sets of keys, the encryption key and the decryption key. The encryption key can be broadcast in public (e.g., published in a phone book) whereas the decryption key has to be kept secret. Public key cryptography allows two parties who have never met before to communicate securely.

Unfortunately, the security of public key encryption schemes is often based on unproven computational assumptions. For instance, the security of standard RSA encryption scheme is based on the presumed hardness of factoring a large composite number. Such an assumption may be broken by unanticipated advances in algorithms and hardware. For instance, in 1994 Peter Shor, then at AT&T, found an efficient quantum algorithm for factoring. [2] Therefore, "if a quantum computer is ever built, much of conventional cryptography will fall apart!" (Gilles Brassard).

You may think, "since we do not have a quantum computer yet, perhaps, we should not worry about this problem until a quantum computer has been built." Not so. For instance, Canada has kept census information secret for 92 years on average. An eavesdropper may save messages sent by you in 2007 and try to decrypt them in 2099. And, who knows whether we will have a quantum computer by 2099?

## II. QUANTUM KEY DISTRIBUTION

It is fortunate that quantum mechanics can also come to the rescue. Unlike conventional cryptography, the Holy Grail of quantum cryptography (code-making) is unconditional security, that is to say, security that is based on the fundamental law of quantum mechanics, namely that information gain generally implies disturbance on quantum states.

How does quantum key distribution work? Intuitively, if an eavesdropper attempts to learn information about some signals sent through a quantum channel, she will have to perform some sort of measurement on the signals. Now, a measurement will generally disturb the state of those signals. Alice and Bob can catch an eavesdropper by searching for traces of this disturbance. The absence of disturbance assures Alice and Bob that Eve almost surely does not have any information about the transmitted quantum signals.

## III. BB84 PROTOCOL: THE IDEAL CASE

The best-known quantum key distribution (QKD) protocol (BB84) was published by Bennett and Brassard in 1984 [3], while its idea goes back to Wiesner. [4] The basic tool are a quantum channel connecting Alice and Bob and a public classical channel, where Eve is allowed to listen passively, but not allowed to change the transmitted message. For the quantum channel, we use four signal states. For simplicity, let us for now regard the signals as realized by single photons in the polarization degree of freedom. Consider two sets of orthogonal signals, one formed by a horizontal and a vertical polarized photon, and the other formed by a 45-degree and 135-degree polarized photon. These four polarized states are non-orthogonal. The overlap probability between signals from two different sets is one half. Bob has two measurement devices at his hand, one in the rectilinear (i.e., vertical/horizontal) basis and one in the diagonal (i.e., 45-degree/135-degree) basis. Notice that Bob's two measurements do not commute.

The procedure of BB84 is as follows. See Figure 1.

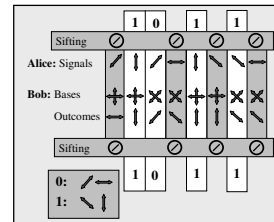


FIG. 1: Schematics of the BB84 protocol. [3]

### 1. Phase I (Quantum Communication Phase)

(a) Alice sends a sequence of signals, each randomly chosen from one of the above four polarizations.

(b) For each signal, Bob randomly chooses one of the two measurement devices to perform a measurement.

(c) Bob confirms that he has received and measured all signals.

### 2. Phase II (Public Discussion Phase)

(a) Alice and Bob announce their polarization bases for each signal. They discard all events where they use different bases for a signal.

(b) Alice randomly chooses a fraction,  $p$ , of all remaining events as test events. For those test events, she transmits the positions and the corresponding polarization data to Bob. Bob compares his polarization data with those of Alice and tells Alice whether their polarization data for the test events agree.

(c) In case of agreement, Alice and Bob convert the polarization data of the remaining set of events into binary form, e.g., they call all horizontal and 45-degree signals

a "0" and all vertical and 135-degree signals a "1". Such a generated binary string is now their secret key.

The first phase of the protocol uses signals and measurements via the quantum channel. Alice keeps a classical record of the signal states she sent. Similarly, Bob keeps a classical record of the measurement devices he has chosen together with his measurement outcomes.

The second phase of the protocol uses a public classical channel. An eavesdropper may try to break the scheme by launching a man-in-the-middle attack where she impersonates as Alice to Bob and impersonates as Bob to Alice. To prevent this attack, Alice and Bob should authenticate the data sent in their classical channel. Fortunately, efficient classical authentication methods exist. To authenticate an  $M$ -bit message, Alice and Bob only need to consume a key of order  $\log M$  bits. In summary, starting from a short pre-shared key, Alice and Bob can generate a long secure key by using quantum key distribution. They can keep a small portion of it for authentication in a subsequent round of quantum key distribution and use the rest as a key for one-time pads. The fact that there is no degradation of security by using this new secure key is called composability and has been proven in [5], provided that one uses a proper definition of security. See, e.g. [5, 6]. As a result, we should strictly speak of QKD as quantum key growing.

The BB84 protocol is only one example of a QKD protocol. Actually, there are many QKD protocols, as nearly any set of non-orthogonal signal states together with a set of non-commuting measurement devices will allow secure QKD. [7] These protocols differ, however, in their symmetry that simplifies the security analysis, in the ease of their experimental realization and in their tolerance to channel noise and loss. Independent of Bennett and Brassard's work, Ekert proposed a QKD protocol (Ekert 91) based on Bell's inequalities [8]. In 1992, Bennett proposed a simple protocol (B92) [9] that involves only two non-orthogonal states. A protocol of particularly high symmetry is the six-state protocol.

#### IV. BB84 PROTOCOL IN A NOISY ENVIRONMENT

The idealized BB84 protocol described above will not work in any practical realizations. Even when there are no eavesdropping activities, any real quantum channel is necessarily noisy due to, for instance, some misalignment in a quantum channel. As a result, Alice and Bob will generally find a finite amount of disturbance in their test signals. Since Alice and Bob can never be sure about the origin of the disturbance, as conservative cryptographers, we should assume that Eve has full control of the channel. Therefore, we are faced with two problems. First, the polarization data of Alice may be different from those of Bob. This means that their raw keys are different. Second, Eve might have some partial information on those raw keys.

In order to address these two problems, Alice and Bob have to perform classical post-processing of their raw keys. First, Alice and Bob may perform error correction to correct any error in the raw key. Now, they share a reconciled key on which Eve may have partial information. Second, they may perform so-called privacy amplification. That is to say, they apply a function on their reconciled key to map it into a final key, which is shorter, but is supposed to be almost perfectly secure.

Proving the security of QKD in a noisy setting was a very hard problem. This is because instead of attacking Alice's signals individually, Eve may conduct a joint attack. In the most general attack, Eve may couple all the signals received from Alice with her probe and evolve the combined system by some unitary transformation and then send parts of her systems to Bob, keeping the rest in her quantum memory. She then listens to all the public discussion between Alice and Bob. Some time in the future, Eve may perform some measurement on her system to try to extract some information about the key. A priori, it is very hard to take all possible attacks into account.

It took more than 10 years, but the security of QKD in a noisy setting was finally solved in a number of papers. In particular, Shor and Preskill [10] have unified the earlier proofs by Mayers [11, 12] and by Lo and Chau [13], by using quantum error correction ideas. [Lo and Chau's proof uses the entanglement distillation approach to security proof, proposed by Deutsch *et al.* [14].] Shor and Preskill showed that BB84 is secure whenever the error rate (commonly called quantum bit error rate, QBER) is less than 11 percent. Allowing two-way classical communications between Alice and Bob, Gottesman and Lo [15] have shown that BB84 is secure whenever the QBER is less than 18.9 percent. Subsequently, Chau [16] extended the secure region up to 20.0 percent. An upper bound on the tolerable QBER is also known: BB84 is known to be insecure when observed correlations contain no quantum correlations anymore [17], which happens when the average QBER is above 25 percent. [18] A major open question is the following: What is the threshold value of QBER above which BB84 is insecure? Is there really a gap between the 20% and the 25%?

#### V. BB84 WITH PRACTICAL SOURCE IN NOISY AND LOSSY ENVIRONMENT

Real-life QKD systems suffer from many type of imperfections. While single photon sources may well be very useful for quantum computing, it is important to note that single photon sources are *not* needed for QKD. This is good news because currently single photon sources are rather impractical for QKD.

(a) Source: It is rather common to use attenuated laser pulses as signals. Those attenuated laser pulses, when phase randomized, follow a Poissonian distribution in the number of photons. i.e., the probability of having  $n$  pho-

tons in a signal is given by  $P_\mu(n) = e^{-\mu}\mu^n/n$  where  $\mu$ , chosen by the sender, Alice, is the average number of photons.

For instance, if we use  $\mu = 0.1$ , then most of the pulses contain no photons, some contain single photons and a fraction of order 0.005 signals contains several photons.

(b) Channel: A quantum channel, e.g. an optical fiber or open air, is lossy as well as noisy.

(c) Detector: Detectors often suffer false detection events due to background and so-called intrinsic dark counts. Moreover, some misalignment in the detection system is inevitable.

Let us consider what happens when we use attenuated laser pulses, rather than perfect single photons, as the source in BB84. [18, 19] The vacuum component of the signal reduces the signal rate since no signal will be detected by Bob. The single photon component of the signal works ideally. The problematic part are the multi-photon signals. Essentially, each multi-photon signal contains more than one copy of the polarization information, thus allowing Eve to steal a copy of the information without Alice and Bob knowing it. More concretely, the presence of multi-photon signals allows Eve to perform the *photon-number-splitting* (PNS) attack. In the PNS attack, Eve performs a quantum non-demolition measurement of the number of photons on each signal emitted by Alice. Such a measurement tells Eve exactly the number of photons in a signal without disturbing its polarization. Now, Eve can act on the signal depending on the total number of photons. If she finds a vacuum signal, she can resend it to Bob without introducing any additional errors. If she finds a multi-photon signal, she splits off one photon and keeps it in her quantum memory and sends the remainder to Bob. Note that when Eve sends the reminder to Bob, she may replace the original lossy quantum channel by a lossless channel. In other words, Eve may effectively introduce photon-number-dependent loss in the channel. Eve's splitting action does not disturb the signal polarization either in the photon she splits off, nor in the photon she sends on. Later in the protocol Alice will reveal the polarization basis of the signal. This will allow Eve to perform the correct measurement on the single photon she split off, thereby obtaining perfect information about the polarization of Alice's signal.

The remaining signals are single-photon signals. Recall that in the PNS attack, Eve has enhanced the transmittance of multi-photon signals by replacing the original lossy quantum channel by a lossless one. Therefore, in order to match the effects of the original loss in the channel, Eve has to suppress some of the single photon signals. That is to say she has to send a *neutral* signal to Bob that will cause no errors and look like loss. Of course, the vacuum signal does this job here. The exact rate of the suppressed signals depends on the mean photon number of the source and the loss in the channel.

On those single-photon signals that she does not block, Eve may perform any coherent eavesdropping attack.

This means that in the worst case scenario, all the errors arise from eavesdropping in single-photon signals.

In the recent years, several groups developed experimental demonstrations of QKD using imperfect devices. QKD experiments have been successfully performed over about 100km of commercial Telecom fibers and also about 100km of open-air. There have even been serious proposals for performing satellite to ground QKD experiments, thus enabling a global quantum cryptographic network through trusted satellites. One fiber-based QKD set-up by the Cambridge group is shown in Figure 2. Fiber-based QKD systems have matured over the recent

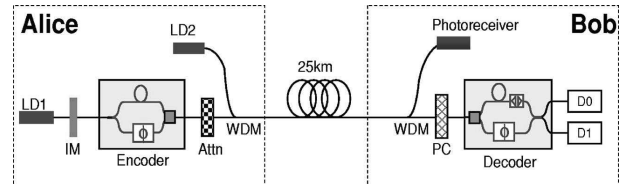


FIG. 2: Schematics of actual QKD experiments with phase-encoding of signals. The figure is from [20] (Courtesy of A. Shields).

years so that at least two firms, id Quantique and MagiQ, manufacture them in a commercial setting.

It is important to notice that a security proof that takes into account all the above imperfections has been given by Gottesman-Lo-Lütkenhaus-Preiskill (GLLP) [21], building on earlier work by Inamori, Lütkenhaus and Mayers [22]. As we pointed out before, it is not "more secure" to use single-photon sources. In fact, at present, it is much more practical to use laser pulses, rather than single-photon sources. Another important issue to mention here is that security proofs assume models for sending and receiving devices (though not for the quantum channel). One has therefore always to check that these models fit the real physical devices.

## VI. NEW METHODS

The rough behaviour of the signal rate according to GLLP is easily understood. For low and intermediate losses, one can ignore the effects of errors, and the secret key rate can be understood in terms of the multi-photon probability of the source,  $p_{multi}$ , and the observed probability that Bob receives a signal,  $p_{rec}$ .

$$G \sim p_{rec} - p_{multi} \quad (1)$$

Assuming a Poissonian photon number distribution for the source with mean photon number  $\mu$ , we find  $p_{multi} = 1 - (1 + \mu) \exp(-\mu)$ , and, assuming that we observe a probability  $p_{rec}$  as in a standard optical transmission with single photon transmittivity  $\eta$  such that  $p_{rec} = 1 - \mu\eta \exp(-\mu\eta)$ , we can perform a simple optimization over  $\mu$  and find the choice  $\mu_{opt} \sim \eta$ . Therefore, we find

$$G \sim \eta^2. \quad (2)$$

This key generation is rather low compared to the communication demand on optical fiber networks. Moreover, due to the detector imperfections, at some point the dark counts of the detectors kick in so that we find an effective cut-off at distances around 20-40 km. In summary, standard implementations of QKD are limited in distances and key generation rates. There are several approaches to solving these problems.

### A. Decoy state QKD

The first and simplest approach is decoy state QKD [23, 24, 25]. In addition to signal states of average photon number  $\mu$ , Alice also creates decoy states of various mean photon numbers  $\nu_1, \nu_2$ , etc. For instance, Alice may use a variable attenuator to modulate the intensity of each signal. Consequently, each signal is chosen randomly to be either a signal state or a decoy state. Given an  $n$ -photon signal, an eavesdropper has no idea whether it comes from a signal state or a decoy state. Therefore, any attempt for an eavesdropper to suppress single-photon signals in the signal state will lead also to a suppression of single-photon signals in the decoy states. After Bob's acknowledgement of his detection of signals, Alice broadcasts which signals are signal states and which signals are decoy states and what types. By computing the gain (i.e., the ratio of the number of detection events to the number of signals sent by Alice) and the QBER of the decoy state, Alice and Bob will almost surely discover such a suppression and catch Eve's eavesdropping attack. As shown by Lo et al. [24], in the limit of infinite number of choices of intensities of the decoy states, the only eavesdropping strategy that will produce the correct gain and QBER for all secretly chosen average photon number is a standard beam-splitter attack. As a result, decoy state QKD allows a dramatically higher key generation rate,  $R = O(\eta)$ , compared to  $R = O(\eta^2)$  for non-decoy protocols as well as a much higher distance for unconditionally secure QKD with a practical QKD system. See Figure 3.

How many decoy states are needed? It has been shown that only one or two type of decoy states are needed for practical protocols. [25, 27] The first experimental demonstrations of decoy state QKD has been done. [28] Given its simplicity, we expect decoy state QKD to become a standard technique in the field. Indeed, many follow-up experiments have now been performed.

### B. QKD with strong reference pulses

The second approach is based on the strong reference pulses idea, dating back to Bennett's 1992 paper. [9] The idea is the following. In addition to a phase modulated weak signal pulse, Alice sends also a strong unmodulated reference pulse to Bob through a quantum channel. Quantum information is encoded in the rela-

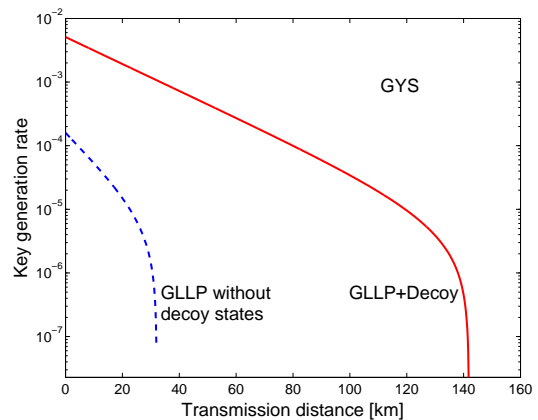


FIG. 3: Key rates for the experimental set-up in [26] using the GLLP results [21] with and without the use of decoy states.

tive phase between the two pulses—the strong reference pulse and the signal pulse. Bob splits off a small part of the strong reference pulse and uses it to interfere with the signal pulse to measure the relative phase between the two. In addition, Bob monitors the intensity of the remainder of each strong reference pulse. Since the reference pulse is strong, such monitoring can be done easily by, for instance, a power-meter.

The idea behind this protocol is to make sure that Eve does not have a neutral signal at her hand which would allow her to suppress signals at will without causing an error rate. (Such a neutral signal plays a crucial role in the PNS attack in addition to the multi-photon signals!) Suppose Eve performs some attacks such as the PNS attack on the signal pulse. For some measurement outcomes, she would like to selectively suppress the signal pulse. But how could she do that?

If Eve significantly suppresses the strong reference pulse, Bob's intensity measurement of the remainder of the strong reference pulse will find a substantially lower value than expected. On the other hand, if Eve does not significantly suppress the strong reference pulse but only suppresses the signal pulse, then when Bob measures the relative phase between the strong reference pulse and the signal pulse, he will find a random outcome (for all conclusive events). So either way, Eve is in trouble.

In a number of recent papers, it has been proven rigorously that QKD with strong reference pulses can achieve a key generation rate  $R = O(\eta)$ . [29, 30] Nonetheless, those proofs require Bob's detection system with certain suitable properties (one proof requires Bob has a local oscillator that has been mode-locked to Alice's strong reference pulse, another requires Bob has a photon detector that can distinguish multi-photon signals from single photons). Therefore, they do not apply to standard "threshold" detectors that do not distinguish single-photon signals from multi-photons.

### C. Differential Phase Shift QKD

A third approach to increase the performance of QKD devices is the differential phase shift (DPS) QKD protocol. [31] Here one uses a coherent train of laser pulses where the bit information is encoded into the relative phase between the pulses. But each pulse belongs therefore to two signals! Though Eve can split photons off the signal trains, these will remain in non-orthogonal signal states and therefore reveal not their *full* information to Eve! (A similar effect exists already in the B92 protocol with a strong reference phase!) In the DPS-QKD protocol Eve is now also hampered again with the suppression of signal states as such a procedure would require to break the pulse train - which causes errors. The same holds for a related scheme using time-bins. [32]

Experimental implementations of DPS QKD have been performed. [33] At present, a rigorous proof of the unconditional security of differential phase shift QKD is still missing.

## VII. CONCLUDING REMARKS

Owing to space limit, we have not talked much about other QKD implementations, such as those based on parametric down conversion sources, nor new detectors such as superconducting single-photon detectors (SSPDs) and transition-edge sensor (TES) detectors. We have omitted also the emerging field of continuous variable QKD systems which make use of homodyne or heterodyne detection.

Security of QKD is a very slippery subject and one should work extremely carefully. Regarding a careful analysis and the formulation of security, see [6]. For nec-

essary and sufficient conditions for security, see [34].

In a popular book, "The Code Book", the author, Simon Singh [35] proposed that quantum cryptography will be the end point of the evolution of cryptography with the ultimate victory of the code-makers. Our view is different. First, quantum cryptography will complement conventional cryptography, rather than replacing it entirely. Second, in order to ensure that a practical QKD system is secure, it is important to verify that the assumptions made in the security proofs actually hold in the practical system. Third, QKD does enjoy a fundamental advantage over conventional cryptography in the sense that, after a quantum transmission, unlike conventional cryptography, there is *no* classical transcript left for the transmission! Therefore, for an eavesdropper to break a QKD system, she has to possess the required quantum technology right at the time of quantum transmission. For this reason, a skillful eavesdropper can and should invest heavily in quantum technology *now*, rather than later, to exploit unexpected loopholes in a practical QKD system. In summary, there is no substitute for battle-testing. We need quantum hackers as much as quantum cryptographers. We live in an exciting time where the interplay between the theory and practice of quantum cryptography has just begun. The everlasting warfare between code-makers and code-breakers continues.

We thank critical comments on the earlier version of this paper by Artur Ekert and Renato Renner. This research is supported by NSERC, CIAR, CRC Program, MITACS, CFI, OIT, PREA, CIPI and Perimeter Institute for Theoretical Physics. Research at Perimeter Institute is supported in part by the Government of Canada through NSERC and the province of Ontario through MEDT.

- 
- [1] D. Welsh, *Codes and Cryptography* (Oxford University Press, 1988).
  - [2] P. W. Shor, SIAM J. Comput. **26**, 1484 (1997).
  - [3] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
  - [4] S. Wiesner, Sigact News **15**, 78 (1983).
  - [5] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, in *Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005.*, edited by J. Kilian (Springer, Berlin, 2005), vol. 3378 of *Lecture Notes in Computer Science*, pp. 386–406.
  - [6] R. Renner, Ph.D. thesis, ETH Zürich (2005).
  - [7] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
  - [8] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
  - [9] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
  - [10] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
  - [11] D. Mayers, in *Advances in Cryptology — Proceedings of Crypto '96* (Springer, Berlin, 1996), pp. 343–357.
  - [12] D. Mayers, JACM **48**, 351 (2001).
  - [13] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
  - [14] D. Deutsch, A. Ekert, R. Josza, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
  - [15] D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003).
  - [16] H. Chau, Phys. Rev. A **66**, 60302 (2002).
  - [17] M. Curty, O. Gühne, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. A **71**, 022306 (2005).
  - [18] G. Brassard, N. Lütkenhaus, T. Mor, and B. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
  - [19] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
  - [20] Z.L. Yuan, A.W. Sharpe, and A.J. Shields, Appl. Phys. Lett. **90**, 011118 (2007).
  - [21] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quant. Inf. Comp. **4**, 325 (2004).
  - [22] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D (2007); quant-ph/0107017.
  - [23] W.-Y. Hwang, Phys. Rev. Lett. **91**, 57901 (2003).

- [24] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
- [25] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
- [26] C. Gobby, Z. Yuan, and A. Shields, Appl. Phys. Lett. **84**, 3762 (2004).
- [27] B. Ma, X. and Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).
- [28] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006).
- [29] M. Koashi, Physical Review Letters **93**, 120501 (pages 4) (2004).
- [30] K. Tamaki, N. Lütkenhaus, M. Koashi, and J. Batuwantudawe, quant-ph/0607082.
- [31] K. Inoue and T. Honjo, Phys. Rev. A **71**, 042305 (2005).
- [32] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Appl. Phys. Lett. **87**, 194108 (2005).
- [33] E. Diamanti, H. Takesue, T. Honjo, K. Inoue, and Y. Yamamoto, Phys. Rev. A **72**, 052311 (2005).
- [34] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).
- [35] S. Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (Doubleday, New York, 1999).